United States Department of Education
Federal Student Aid

Student Aid Internet Gateway (SAIG)
Continuity of Support/ Disaster Recovery Plan

FINAL DRAFT
December 19, 2002

1.0 INTRODUCTION

Continuous risk management will identify and mitigate most system and facility vulnerabilities to the Student Aid Internet Gateway (SAIG). However, even after mitigating risks through managerial, operational, and technical controls, it is improbable that all risk inherent to the system could ever be eliminated. Preparing for contingencies, including documenting procedures, testing plans, and training contingency planning team members, is an essential component of operating and maintaining SAIG despite any remaining risk.

SAIG relies on the Virtual Data Center (VDC), operated by Computer Sciences Corporation (CSC), as its general support system. The VDC provides the hardware and network connectivity that allows SAIG to perform its business functions. CSC has the lead in the recovery of SAIG during a system disruption or disaster. The FSA Integration Partner maintains the SAIG software, and performs troubleshooting support during system recovery.

Per the Department's guidance in its IT Contingency Planning Guide, the SAIG Continuity of Support and Disaster Recovery Plans have been combined into one document (hereafter referred to as the SAIG/DR Plan). The Department recommends including a disaster recovery plan with the continuity of support plan for Tier 3 and 4 systems.

1.1 Purpose

The purpose of this plan is to identify and document the Continuity of Support and Disaster Recovery procedures for the consistent operation of SAIG in the event of a disruption at the VDC. The following objectives have been established for this plan:

- Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:
    - ***Notification/Activation phase*** to detect and assess damage and to activate the plan
    - ***Recovery phase*** to restore temporary IT operations and recover damage done to the original system
    - ***Reconstitution phase*** to restore IT system processing capabilities to normal operations.
- Identify the activities, resources, and procedures needed to carry out SAIG processing requirements during prolonged interruptions to normal operations.
- Assign responsibilities to designated FSA and contractor personnel and provide guidance for recovering SAIG during prolonged periods of interruption to normal operations.
- Ensure coordination with other organizations' staff who will participate in the contingency planning strategies as well as external points of contact and vendors who will participate in the contingency planning strategies.

1.2 Applicability

The SAIG COS/DR Plan applies to the functions, operations, and resources necessary to restore and resume FSA's SAIG operations as it is installed at CSC's VDC in Meriden, CT. The SAIG COS/DR Plan applies to FSA and all other persons associated with SAIG as identified under Section 2.4, Responsibilities.

The SAIG COS/DR Plan is supported by the *VDC Disaster Recovery Plan for the Department of Education Midrange Platforms*, which provides the Disaster Recovery procedures for all systems supported by the VDC. This plan will not detail every procedure in the VDC DRP, but will provide sufficient information to convey the notification, recovery, and reconstitution procedures employed by organizations supporting SAIG.

1.3 Scope

The scope of this plan is two-fold. First, to identify the COS/DR teams responsible for the continued operation of SAIG during a system disruption. Second, to establish recovery procedures that will minimize the loss of SAIG productivity during system disruptions.

Various scenarios were considered to form a basis for this plan, and multiple assumptions were made. The applicability of the plan is predicated on two key principles –

- The VDC facility in Meriden, CT, is inaccessible; therefore, CSC is unable to perform SAIG processing for FSA.
- A valid contract exists with the alternate site that designates the site in Carlstadt, NJ, as CSC's alternate operating facility.
  - CSC will use the Sungard building and IT resources to recover SAIG functionality during an emergency situation that prevents access to the original facility.
  - The designated computer system at the alternate site has been configured to begin hosting SAIG.
  - The alternate site will be used to continue SAIG recovery and processing throughout the period of disruption, until the return to normal operations.

Based on these principles, the following assumptions were used when developing the SAIG COS/DR Plan–

- SAIG is designated as inoperable at the VDC if it cannot be recovered within 24 hours.
- Key SAIG personnel have been identified and trained in their emergency response and recovery roles; they are available to activate the SAIG COS/DR Plan.
- Key SAIG personnel from CSC and the Integration Partner will be available to activate the SAIG COS/DR Plan.
- Preventive controls (e.g., generators, environmental controls, waterproof tarps, sprinkler systems, fire extinguishers, and fire department assistance) are fully operational at the time of the disaster.
- Computer center equipment, including components supporting SAIG, is connected to an uninterruptible power supply (UPS) that provides 45 minutes to 1 hour of electricity during a power failure.

- SAIG hardware and software at the VDC are unavailable for at least 24 hours.
- Current backups of the application software and data are intact and available at the Iron Mountain offsite storage facility.
- The equipment, connections, and capabilities required to operate SAIG are available at the alternate site in Carlstadt, NJ.
- Service agreements are maintained with SAIG hardware, software, and communications providers to support the emergency SAIG recovery.
- The SAIG HP/UX and NT servers are considered level 1 priority by the VDC and its alternate facility. [1]
- All EAI recovery procedures are contained in an EAI COS/DR Plan.

The SAIG Contingency Plan does not apply to the following situations:

- **Overall recovery and continuity of business operations.** This plan does not describe the Business Resumption Plan (BRP) and Continuity of Operations Plan (COOP) maintained by the Department of Education, Office of the Chief Information Officer.
- **Emergency evacuation of personnel.** This plan does not describe Occupant Evacuation Plan (OEP). This plan is the responsibility of the organizations hosting, developing, and maintaining SAIG.

1.4 References/Requirements

This SAIG COS/DR Plan complies with the *FSA's* IT contingency planning policy identified below:

> *FSA's Contingency Plan policy defines the emergency operating procedures that must be followed to make sure FSA's critical functions continue to operate and support IT systems in the event of disruptions, both large and small. Emergency procedures must have timelines for recovery and restoration of specified services prioritized by the system's mission criticality. FSA must regularly review and test backup and restoration procedures…. FSA must make sure that a comprehensive contingency and disaster recovery plan is in place and tested for each system on the basis of this prioritization. These plans must have detailed procedures for restoring operation of the system, including the personnel responsible and the timeline within which the FSA system must be returned to normal business operations*

This plan is based on the template provided in NIST Special Publication 800-34: Contingency Planning Guide for Information Technology Systems. The SAIG COS/DRP also used the following Federal and Education policies:

- The Computer Security Act of 1987
- OMB Circular A-130, *Management of Federal Information Resource*s, Appendix III, November 2000.
- Federal Preparedness Circular (FPC) 65, *Federal Executive Branch Continuity of Operation*s, July 1999

[1] VDC DR Plan section 8.3.1

- Presidential Decision Directive (PDD) 67, *Enduring Constitutional Government and Continuity of Government Operation*s, October 1998
- PDD 63, *Critical Infrastructure Protectio*n, May 1998
- Federal Emergency Management Agency (FEMA), *The Federal Response Plan (FRP*), April 1999
- Defense Authorization Act (Public Law 106-398), Title X, Subtitle G, "Government Information Security Refor*m*," October 30, 2000
- NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, June 2002.
- Department of Education IT Contingency Planning Guide
- FSA IT Security and Privacy Policy.

1.5 Record of Changes

Modifications made to this plan since the last printing are as follows:

Page No(s).	Change Comments	Date of Change	Author
Entire document	**Original Plan Creation – Final Draft**	**12/3/2002**	**Mod Partner**

2.0 CONCEPT OF OPERATIONS

2.1 System Description and Architecture

The Student Aid Internet Gateway (SAIG) provides telecommunications support for the delivery and administration of Title IV programs via the Internet. The portal consists of HP-UX mid tier servers (production and development), which host the following applications:

- TD Engine – An open architecture gateway that is used as the 'mailbox' application for the storing and retrieval of data.
- TDAccess – The client software used to send and receive FSA data transmissions securely over the Internet using SSL 3.0 and the Diffie-Hellman Dynamic Key Exchange algorithm.

In addition, a Windows NT 4.0 server hosts the TD Community Manager (TDCM) application. TDCM is used to view the header and footer of mailbox messages but not the content.

Computer Sciences Corporation (CSC) runs these components from the Virtual Data Center VDC. CSC staff is responsible for the operation, maintenance, and security of SAIG with remote application support provided by Accenture and NCS Pearson. See Appendix D for the SAIG logical system diagram.

2.2 Line of Succession

FSA sets forth an order of succession to ensure that decision-making authority for the SAIG COS/DR Plan is uninterrupted. The FSA Chief Information Officer (CIO), in coordination with CSC's Manager of Contingency Services, is responsible for ensuring the safety of personnel and the execution of procedures documented within this SAIG COS/DR Plan. If the CIO is unable to function as the overall authority or chooses to delegate this responsibility to a successor, an appropriate Deputy CIO shall function as that authority.

2.3 Disaster Definition

CSC defines a disaster as an event that significantly reduces the ability of the VDC to provide normal data processing services for more than 24 hours. The VDC determined the following events to be the most likely to occur at the VDC:

Natural

- Earthquake
- Storm Damage
- Lightening
- Flood
- Hurricane

Man-made

- Terrorist attack
- Internal Sabotage
- Human error
- Vandalism
- Toxic Chemicals Contamination
- Plane Crash

- Communication Loss

Physical

- Power Loss/Surge
- Fire
- Explosion
- Structural Failure (External and Internal)
- Hardware Failure
- Loss of Water Supply

The VDC uses two disaster modes to determine which recovery plan to enact. The table below describes the important components of each disaster mode.

	Required downtime	Alternate Site
Disaster Mode A	Less than 24 hours	No
Disaster Mode B	More than 24 hours	Yes

CSC uses Disaster Mode A to respond to contingencies such as water pipe breakage, server failure and loss of telephone service. Disaster Mode B responds to contingencies such as structural collapse or total hardware failure. For SAIG, Disaster Mode A refers to the Continuity of Support procedures contained in the plan. Disaster Mode B refers to the Disaster Recovery procedures

2.4 Responsibilities

The following CSC teams[2] have been developed and trained to respond to a contingency event affecting, among other systems, SAIG:

- Contingency Planning Committee
- Service Restoration Team
- Disaster Recovery Team

Additionally, the Mod Partner contributes several supporting roles in a contingency response scenario.

2.4.1 Contingency Planning Committee

The Contingency Planning Committee (CPC) consists of personnel from the following areas[3]:

- Computer Sciences Corporation
- CSC Account Management
- FSA CIO.

The Committee is responsible for developing, documenting and testing the Disaster Recovery Plan and for coordinating training activities within their individual functional areas. The Manager of Contingency Services is chairperson of the CPC and also chairperson of the Disaster Recovery Team.

[2] For a detailed description of the CSC teams participating in disaster recovery, refer to appendix A
[3] Section extracted in part from VDC Disaster Recovery Plan for Midrange Systems dated March 8, 2002

2.4.2 Service Restoration Team

When a critical problem is not resolved within 6 hours, CSC implements its Service Restoration process[4]. The process serves as a communication vehicle between cross-functional groups forming the Service Restoration Team (SRT) and stresses the importance of effective restoration and escalation processes. Their first priority is to complete a brief evaluation of the critical problem. The SRT, along with members of the Disaster Recovery Team, is tasked with conducting an in-depth damage assessment. Depending on the type of problem, there may be a danger to personnel and/or damage to the facility that would necessitate a restoration of processing at another location.

Based on this assessment, a recommendation is made to activate the Disaster Recovery Plan at the appropriate disaster mode and coordinate the Disaster Recovery Team's execution of the plan. The SRT will then inform the CSC Directors of their recommendation for the Virtual Data Center. Concurrent with performing their evaluation procedures, SRT members are responsible for initiating and monitoring recovery tasks assigned to their functional areas. The Service Restoration Team (SRT) consists of personnel from the following areas:

- Virtual Data Center Manager (SRT Chairperson)
- Performance Tuning Capacity Planning Manager
- Manager of Technical Services
- Manager of Network Services
- Business Continuity and Contingency Services Manager
- Manager of Security
- Manager of Facility Services
- Vice President in charge of Customer Accounts
- Virtual Data Center Human Resources Director
- Regional Account Manager
- Vendor Representatives

2.4.3 Disaster Recovery Team

The members of the Disaster Recovery Team (DRT) are responsible for maintaining contingency preparedness plans on a daily basis as part of the normal operating procedures within their functional areas.[5] They are also responsible for implementing recovery procedures after the Manager of Contingency Services formally declares a disaster and activates the Disaster Recovery Plan.[6] The Manager of Contingency Services functions as the Chairperson of the Disaster Recovery Team. Team members must keep FSA, as well as their SRT representatives, informed of the status of these recovery activities and ensure that they are maintained or completed.

In addition to the SRT members, the Disaster Recovery Team consists of key personnel from each functional area listed below:

---

[4] Section extracted in part from VDC Disaster Recovery Plan for Midrange Systems dated March 8, 2002
[5] Section extracted in part from VDC Disaster Recovery Plan for Midrange Systems dated March 8, 2002
[6] For a list of persons authorized to declare a disaster, refer to appendix B.

- CSC Technical Personnel (Operations, Teleprocessing, Technical Services)
- CSC Human Resources
- CSC Security Personnel
- CSC Facilities Personnel
- CSC Finance
- Vendor Representatives
- CSC Customer Management.

2.4.4 Mod Partner Personnel

In the unlikely event that key Mod Partner personnel are unable to react during a contingency, Mod Partner has in place procedures to ensure that essential tasks and operations will continue uninterrupted. The first line of defense is the individual's immediate supervisor. The immediate supervisor is responsible for verifying that duties of key individuals continue to be performed with no loss in SAIG operational capability. Mod Partner staff has a backup strategy identified in the table below.

Position	First Backup	Second Backup
Program Manager	Business Unit Director	Processing System Manager
Database Administrator	System Administrator	Backup System Administrator
Software Development Manager	System Administrator	Secondary Backup Administrator

2.5 Plan Distribution

Distribution of the SAIG COS/DR Plan is restricted to select individuals as indicated in the Distribution List below[7].

Name	Organization	Email	Telephone
Lydia Morales	FSA	Lydia.morales@ed.gov	202-377-3589
Baha Shehata	FSA	Baha.shehata@ed.gov	202-377-3574
Tawanda Hampton	FSA	Tawanda.Hampton@ed.gov	202-377-3575
Colleen Ward	Accenture	Colleen.m.ward@accenture.com	703-947-2980
Frank Southfield	ICS	Frank.southfield@icsc1.com	202-962-0790
Justin Thoenson	NCS Pearson	Justin_Thoeson@ncs.com	319-665-7809
Gary Adams	CSC	gadams2@csc.com	202-842-8614

2.6 Plan Testing

The FSA, Mod Partner and CSC will review the SAIG COS/ DR Plan and SAIG portions of the VDC DRP on an annual basis. Disaster recovery testing at the VDC will take place a minimum of once a year. The VDC will use alternate processing facilities located in Carlstadt, New Jersey to support its disaster recovery requirements.

[7] Appendix F contains a complete listing of SAIG points of contact.

The VDC provides a plan to recover computer systems to the extent that they are covered under the terms of existing contracts. Portions of the VDC Disaster Recovery Plan will be reviewed and updated after each disaster recovery test; however, the entire plan will be reviewed and updated annually. The SAIG COS/DRP will be reviewed and updated annually as well.

2.6.1 Testing Methodology

The CSC Manager of Contingency Services schedules annual simulation tests for SAIG at the hot-site facility.[8] The tests will include, but are not limited to, the following:

- Retrieval and transport of all necessary programs and data from the off-site storage facility to the hot-site,
- Recovery of the operating system to run at the hot-site,
- Establishment of communication networks between the hot-site and the user community,
- Execution of at least one batch and one on-line application, and
- Verification of procedures and test plans for each environment.

Test plans[9] contain detailed lists of tasks that include configuring the hardware and communication links, initializing and restoring databases, testing on-line networks, and generating output. Throughout a test, the amount of time required to complete the task will be recorded. Comments will also be included, as required, for review at the post-test session.

The results of all tests are reported to the CSC Director of Contingency Services, FSA Account Management and the SAIG System Manager. Assigned action items resulting from testing are completed prior to subsequent testing.

2.6.2 Recent Test

On November 12, 2002, FSA performed a Disaster recovery test on SAIG. CSC conducted the hotsite disaster recovery test at the Sungard hotsite recovery facility in Carlstadt, New Jersey. The test included SAIG Mailboxing, SAIG Enrollment, FSA Download, and the Production systems residing on the HP and NT servers. The HP midrange recovery began at 0800 hrs, November 12, and ended before 0800 hrs on November 14. The HP recovery test was a “48 hour” test. The NT Midrange recovery began at 2400 hrs, November 12 and ended before 0800, November 14. The NT recovery test was a “32 hour” test. A list summarizing the SAIG recovery test’s primary objectives is located in Appendix C.

2.7 Plan Maintenance

In order to ensure that all team members have an accurate and current copy of the COS/DR Plan, all changes and revisions must be processed through the SAIG System Manager and distributed to all members on the SAIG COS/DR Plan distribution list. Updates to the plan will be made annually or on an "as needed" basis.

[8] Section extracted in part from VDC Disaster Recovery Plan for Midrange Systems dated March 8, 2002
[9] Appendix C contains the November 2002 test schedule for SAIG.

3.0 CONTINUITY OF SUPPORT AND DISASTER RECOVERY STRATEGIES

Continuity of Support and Disaster Recovery occurs in three distinct phases: Notification/Activation, Recovery, and Reconstitution. During the Notification/Activation phase, recovery personnel are notified via call trees of a system disruption or emergency. A Damage Assessment team determines the extent of the damage and the estimated recovery time. A Manager of Contingency Services determines whether to implement the COS or DR Plan. The recovery phase procedures execute temporary IT processing capabilities in order to repair the damage to the original system and/or restore operational capabilities at the original or new facility. During reconstitution, the system's normal operations are transferred back to the organization's facility and recovery activities are terminated.

In the event of a potential or actual disaster at the VDC, either the CSC Help Desk or the CSC Building Security will notify the Service Restoration Team to assess the damage and report to the VDC Data Center Manager or alternate.

The SRT members are notified, and, with the help of vendor representatives, will prepare a detailed damage report containing the estimated cost and time required to restore services at the Meriden facility. If the VDC Data Center Manager declares a disaster and activates the hot-site, the Manager of Contingency Services will notify the off-site storage facility to ship the application/database files and documentation to the hot-site. Upon arrival at the hot-site, the VDC Disaster Recovery Team will restore the affected production environment(s) and establish the communication network(s).

Once the original site or new site have been established and tested, system operations are transferred from the hot site to the permanent location.

3.1 VDC Continuity of Support/Disaster Recovery Objectives

The VDC achieves its Continuity of Support and Disaster Recovery objectives by:[10]

- Providing the information and procedures necessary to respond to an occurrence, notify key recovery personnel, assemble recovery teams, and recover data processing at the current or alternate site within 24 hours after a disaster has been declared.

- Creating a disaster recovery structure strong enough to provide guidance to all interrelated groups, yet flexible enough to allow CSC personnel to respond to whatever type of disaster may occur.

- Providing specific action plans for each CSC functional area both to prevent an accidental occurrence of a disaster and to respond effectively during an emergency situation.

- Identifying those activities necessary to resume full services at the reconstructed disaster site or new permanent facility.

[10] Section extracted in part from VDC Disaster Recovery Plan for Midrange Systems dated March 8, 2002

- Testing the recovery procedures annually using the hot-site facility and data stored off-site.

The VDC has and continues to implement preventive measures that are intended to reduce the exposure and or limit damage in the event of a disaster. These measures include periodic test and inspection of the Uninterrupted Power Supply (UPS), diesel generators, sprinkler system, Halon A/C, mechanical and electrical systems. Such measures alone, however, do not completely eliminate the potential of a disaster happening and, therefore, a plan is in place to resume operations with a minimum disruption to SAIG and other VDC-hosted interconnected systems.

The VDC provides a plan to recover computer systems to the extent that they are covered under the terms of existing contracts. Portions of the VDC Disaster Recovery Plan will be reviewed and updated after each disaster recovery test; however, the entire plan will be reviewed and updated annually.

The VDC will review SAIG portions of the VDC DRP on an annual basis. Disaster recovery testing at the VDC will take place a minimum of once a year. The VDC will use alternate processing facilities located in North Bergen and Carlstadt, New Jersey or Wood Dale, Illinois to support its disaster recovery requirements.

3.2 Mod Partner Continuity of Support/Disaster Recovery Objectives

In the event of a disaster, Mod Partner will be guided by its Disaster Recovery Team. The Team will analyze the situation as to the extent of damages, review the recovery plan, and commence the recovery operation. Under the direction of the team leader, NCS Pearson's recovery teams will take the following actions:

- Contact all DRT members and establish a time and place for the team to meet, preferably at the location site.
- Make a preliminary written assessment in order to report to other team members who will concentrate on their particular areas of responsibility.
- The NCS Manager of Client Support Services, along with Computer Operations shift managers and Computer Operations lead operators will coordinate the staffing and operation at the recovery site; contact appropriate vendors; and coordinate replacement orders.
- The NCS Software Team leader, along with Technical Support members, will bring up the necessary operating system software at the recovery site and provide technical support to the application, operations, and data communications team as required.

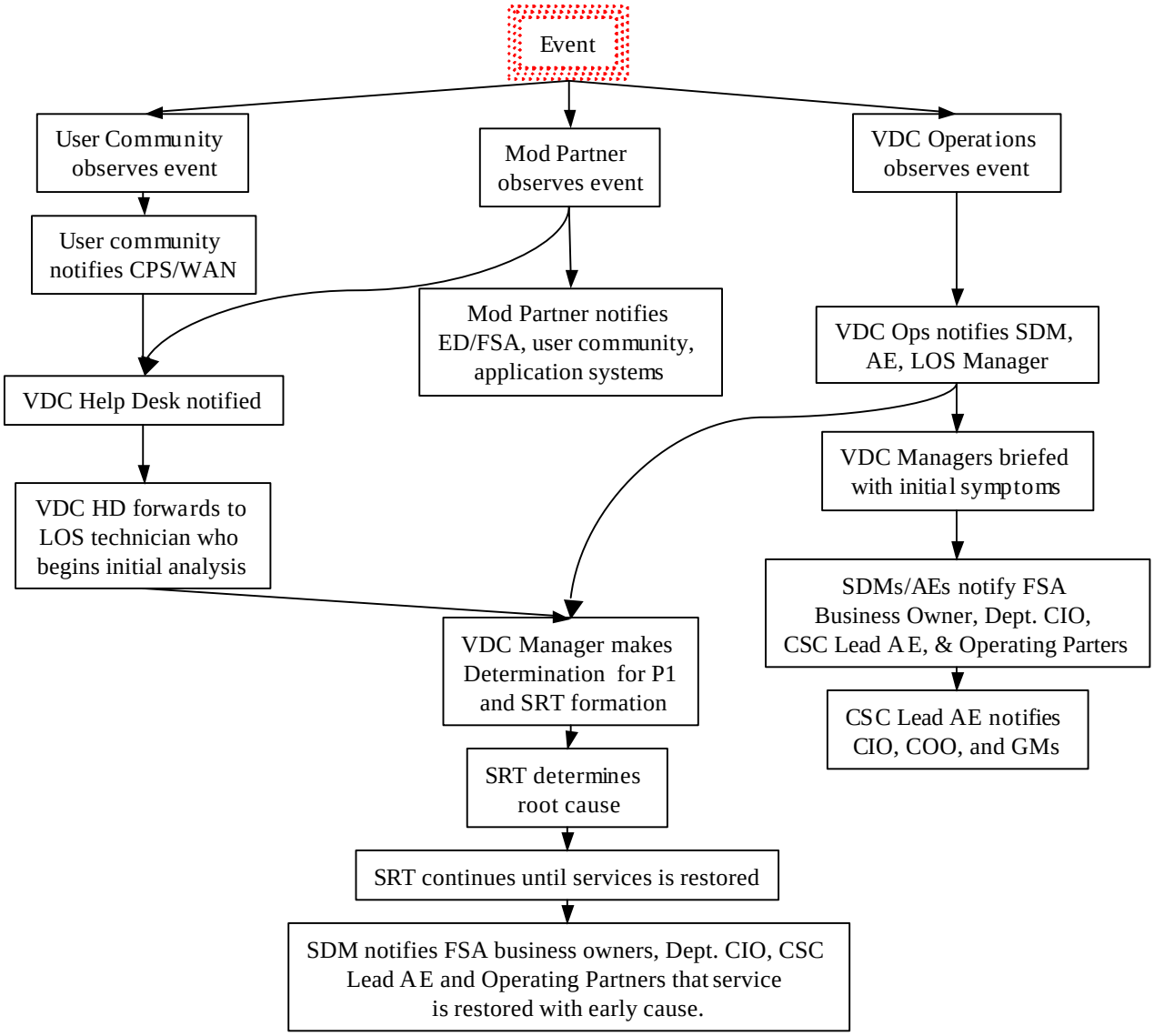
3.3 Notification and Activation

This phase addresses the initial actions taken to detect and assess damage inflicted by a disruption to SAIG. Based on the assessment of the event, the plan may be activated by the CSC Manager of Contingency Services.[11]

3.3.1 COS/DR Notification

The initial disaster response procedure is based on the assumption that damage will disable the data center for more than 24 hours. If recovery is possible in less than 24 hours, normal computer processing, aided as necessary by a Service Restoration Team, will resume as quickly as possible. The VDC uses consistent application recovery procedures for all of its hosted applications. The process flow below describes how the SAIG operating partners respond to an event affecting SAIG processing. The initiation of the process can be activated by numerous sources, namely the user community, Mod Partner, or VDC Operations.

[11] Note: In an emergency, CSC's top priority is to preserve the health and safety of its staff before proceeding to the Notification and Activation procedures.



COS Notification Process

Initial response procedures to a contingency will be initiated within six (6) hours after the event occurred. The major steps that take place within this timeframe are listed below:[12]

Event + 1 Hour (To be handled by Building Security and CSC Facilities staff)

- Execute emergency and evacuation plans
- Secure damaged area
- Notify fire and security departments
- Notify Service Restoration Team. (To be handled by Building Security or Help Desk)

Event + 1-4 Hours (To be handled by the SRT)

- Assemble Service Restoration Team at damaged site

[12] Section extracted in part from VDC Disaster Recovery Plan for Midrange Systems dated March 8, 2002

- Contact Regional Account Executive
- Put hot-site on stand-by
- Put off-site storage on stand-by
- Put telecommunications provider on stand-by to activate communications capability
- Perform preliminary damage assessment.

Event + 4-6 Hours
- Determine if the hot-site will be used
- If no,
- Continue normal problem response procedures, else activate hot-site
- If yes,
- Notify off-site storage facility to ship tapes to hot-site
- Notify telecommunications provider to activate necessary network lines
- Select command center location
- Assemble all Disaster Recovery Team members.

Event + 6 ~ Hours
- Start detailed damage assessment procedures
    - Implement Disaster Recovery Plan.

3.3.2 SRT Notification

The CSC Service Restoration Team consists of, but is not limited to, the following positions: Manager of Contingency Services and Chairperson, VDC Manager, VDC Manager of Contingency Services, Manager of Security, and HR Director.[13] When contacted, the SRT members are given the following information:

- Time the disaster occurred
- A brief description of what happened and the areas affected
- Where and when to assemble with other SRT members
- When to contact staff and what to tell them.

Although the VDC Disaster Recovery Plan assigns specific responsibilities to each person, available management personnel will perform the initial response procedures as quickly as possible.

3.3.3 DRT Notification

The Disaster Recovery Team consists of the Service Restoration Team members (who serve as the team leaders on the Disaster Recovery Team) and key personnel within each functional area (e.g. Unix Midrange Manager).[14] The team leaders will be responsible for notifying the other members on his/her team and provide the following information:

- Notification of the disaster
- Disaster mode declared
- Which hot-site will be used
- Location of the command center

[13] Section extracted in part from VDC Disaster Recovery Plan for Midrange Systems dated March 8, 2002
[14] Section extracted in part from VDC Disaster Recovery Plan for Midrange Systems dated March 8, 2002

- Where and when to report.

If Disaster Mode B is declared, the DRT Chairperson instructs key personnel to prepare to travel to the hot-site.

3.3.4 FSA Notification

During an event, Gary Adams, the CSC Service Delivery Manager for SAIG (among other FSA systems) will notify the FSA SAIG Technical Manager Lydia Morales, Mod Partner Manager Colleen Ward, FSA VDC Manager Keith Wilson, and NCS Pearson. Ms. Morales will notify Baha Shehata and the SSO Tawanda Hampton. Colleen Ward will notify Paul Peck (direct supervisor) and Robert O'Keefe (Mod Partner Partner-in-Charge).

3.3.5 Hot-Site Facility Notification

The Manager of Contingency Services will notify Sungard to be on the alert if there is an indication that the hot-site will be needed.

When the Meriden Service Delivery Manager authorizes the use of the hot-site, the Manager of Contingency Services or alternate calls Sungard to inform them that a disaster has been officially declared and CSC will use their facility. When Sungard receives the official disaster declaration, they will confirm that the recovery facility will be turned over to CSC/Meriden personnel within twenty-four (24) hours.

3.4 Recovery

This plan contains procedures for the recovery of SAIG for multiple contingencies. Section 3.2.1 describes the recovery procedures for contingencies that do not require relocation to an alternate site. Section 3.2.2 describes the recovery procedures for a disaster contingency, requiring the relocation to an alternate site.

3.4.1 Continuity of Support Recovery Procedures

Reactive contingency involves a reaction to an unplanned event such as unexpected software corruption. Mod Partner and CSC will work closely with FSA to ensure that it will have anticipated, as closely as possible, all fluctuations in service. When circumstances beyond the control of the contractors occur, they will be prepared to react quickly to an unplanned event. The following list of activities will be implemented as soon as possible:

- Determine the scope of the event or requirements
- Develop a recovery schedule
- Apply appropriate resources to respond to the event
- Apply quality control measures to ensure proper recovery
- Provide ongoing program management and monitoring

The table below describes numerous contingencies that could affect the consistent operation of SAIG at the VDC. The table includes the occurrence name, a description of the risk, existing safeguards, and the initial action taken by the appropriate group or individual.

Natural Contingencies			
Occurrence	**Risk**	**Safeguard**	**Initial Action**
Flood	The VDC does not reside in a flood plain, but the risk of flood, while small, is still a risk.	The Data Center was not built in a flood plain, reducing the risk. Additionally, SAIG operates on a raised computing platform.	Physical security incidents are reported to the on-site VDC Security Officer for validation as per *VDC Security Investigation Procedure*.
Windstorm/Hurricane/ Tornado	Although the likelihood of these events occurring is not high, the Meriden, CT area has been subject in the past to heavy storms, including wind storms, hurricanes and tornadoes.	CSC personnel have the ability to operate and monitor VDC system's remotely. Short-term physical access restrictions will not disrupt SAIG operations.	Security personnel would announce building evacuation using procedures similar to "Fire/Smoke Alarm Response Procedure #1 Section #2"
Earthquake	The US Geological Survey, Earthquake & Volcano Section, assesses the likelihood of heavy tectonic activity in Meriden, CT as highly unlikely.	Based on the low risk and the high costs associated, no earthquake safeguards are provided. Evacuation and personnel safety would be the primary objective.	Security personnel would announce building evacuation using procedures similar to "Fire/Smoke Alarm Response Procedure #1 Section #2"
Winter Storm	Large winter storms, including blizzards and ice storms, happen with moderate regularity. Such storms could prevent personnel from getting to work, as well as compounding other incidents by delaying emergency or maintenance personnel.	CSC personnel have the ability to operate and monitor VDC system's remotely. Short-term physical access restrictions will not disrupt SAIG operations.	Physical security incidents are reported to the on-site VDC Security Officer for validation as per *VDC Security Investigation Procedure*.

Environmental Contingencies			
Occurrence	**Risk**	**Safeguard**	**Initial Action**
Fire	Local or facility-wide fire could cause severe human and computer damage resulting in loss of life and system down-time	Smoke detectors, Fire detectors, Sprinklers (dry),	Security personnel would announce building evacuation using procedures similar to "Fire/Smoke Alarm Response Procedure #1 Section #2"
Loss of Electricity/ Power Surge	Due to the significant power demands of the VDC, loss of electricity could severely hamper the continuity of VDC	In the event of a power failure, battery power is available to provide immediate electrical service until the	Automatic implementation of fail-over recovery procedures followed by root cause analysis

	support to FSA	generators are fired. The battery room consists of two banks of 250 batteries each. The engine room houses three 1,400-kilowatt Bell Detroit diesel generators. A 150-gallon day tank, located in the engine room, fuels each generator. The day tank feeds off two 20,000-gallon underground fuel tanks. The generator room has the capacity for two more generators of equal size should the computer capacity of the building warrant increased generator capacity.	
Heating, Ventilation, Air Conditioning	The failure of the HVAC system could make working conditions unbearable for employees. Additionally, computer hardware exposed to extreme temperatures could cause system failure.	Two Cleaver Brooks gas-fired hot-water boilers provide heat to the center. Cooling is provided by three York chillers with a capacity of 450 tons each. Two cooling towers on the roof of the building support the chillers. Four pumps control the chilled water flow and supply the computers with chilled water. The computer room environment is serviced by 18 Liebert units, which are tied into the chilled water loop.	Automatic implementation of fail-over recovery procedures followed by root cause analysis
Loss of Telephone Service	Decreased person to person communication capability among operating partners (VDC, Integration Partner, FSA)	Communicate via email and paging.	CSC will implement its call-out procedures to inform key individuals and partners of the loss of telephone service.
Loss of Water/Sanitary Facilities	Loss of water could impact the HVAC system, resulting in HVAC failure. HVAC failure impacts both personnel and computer hardware.	The HVAC chillers require a significant water supply, which is met by a combination of city water and an on-site well. The city supply is used for the domestic and fire protection requirements, while the	CSC will implement its HVAC backup procedures. FSA and operating partner notification will occur only if SAIG processing is impacted.

		cooling towers derive their supply from the well. In order to satisfy any contingency planning, the water supplies are fully interchangeable.	
Water Pipe Breakage/ Sprinkler Discharge	Water damage to computer systems could cause local system failure.	The VDC does not have water in the pipes unless an emergency is occurring.	SRT would determine extent of damages; if repairs would exceed 12 hours, DRP procedures would ensue. Else, actions would follow those related to affected subcomponents.
Structural Failure (Internal/External)	Partial or complete structural collapse of the building could damage system components, environmental support systems, or facility personnel.	The VDC is an ISO 9000 certified facility and meets all building code requirements, thus diminishing the probability for structural collapse.	SRT would determine extent of damages; if repairs would exceed 12 hours, DRP procedures would ensue. Else, actions would follow those related to affected subcomponents.

Deliberate Contingencies			
Occurrence	**Risk**	**Safeguard**	**Initial Action**
Bomb Threat	Employee evacuation could cause system disruption or processing delays	CSC employees are trained to handle bomb threats. Detailed procedures exist within the VDC security plan to handle this contingency.	Follow "Bomb Threat Emergency Procedure #1 Section #2". Take notes regarding conversation, and turn over all information to Data Center Security.
Sabotage	Could result in component failures, data corruption, damage to facility	Data integrity procedures within the SAIG system and throughout interconnected Title IV systems.	Depending on extent of damage to the facility, security personnel will announce VDC evacuation. For component failure or data corruption, follow normal notification and recovery procedures (sec. 3.3.1).
Fire/Arson	Local or facility-wide fire could cause severe human and computer damage resulting in loss of life and system down-time	Smoke detectors, Fire detectors, Sprinklers dry	Depending on extent of damage to the facility, security personnel will announce VDC evacuation. For component failure or data corruption, follow normal notification and recovery procedures (sec. 3.3.1).
Cyber Attack – External	Compromise data confidentiality, integrity,	Multiple layers of security including	All computer and network related security

	or availability	firewall, NATed subnet, IDS, etc.	incidents are reported to the CSC Computer Emergency Response Co-ordination Center (CERCC) and up the CSC management chain as per GISS Policy 19 SP-I013 Virus Protection Plan as well as Federal Computer Incident Response Center (FedCIRC) and FSA VDC Security Officer.
Cyber Attack - Internal	Compromise data confidentiality, integrity, or availability	Background investigations on CSC, FSA, Mod Partner employees. Access to data while within SAIG limited because data is compressed and encrypted.	All computer and network related security incidents are reported to the CSC Computer Emergency Response Co-ordination Center (CERCC) and up the CSC management chain as per GISS Policy 19 SP-I013 Virus Protection Plan as well as Federal Computer Incident Response Center (FedCIRC) and FSA VDC Security Officer.

Component Failure Contingencies			
Occurrence	**Risk**	**Safeguard**	**Initial Action**
Loss of NT Server	Failure of users to access TD Community Manager	Co-located backup/test server configured identically to production	Switch failed production server to co-located fail-over server. Conduct root cause analysis.
Loss of Unix Server	Failure of Mailboxing application.	Co-located backup/test server configured identically to production	Switch failed production server to co-located fail-over server. Conduct root cause analysis.
Loss of Communication Lines	Failure of access to TD Community Manager and Mailboxing application	Multiple redundant communication lines reduce the risk of total communication line failure	Transfer communication from failed communication line to operational comm. line.

3.4.2 Disaster Recovery Procedures

This section provides procedures for recovering the application at the alternate site, whereas other efforts are directed to repair damage to the original system and capabilities. Each procedure should be executed in the sequence it is presented to maintain efficient operations.

Detailed SAIG recovery procedures, such as hardware configurations, script execution procedures, and individual personnel recovery responsibilities are detailed in the *VDC Midrange Disaster Recovery Plan* and will not be duplicated or maintained in the SAIG COS/DR Plan.

When the Meriden Data Center Manager authorizes the use of the recovery site, the VDC Manager of Contingency Services is responsible to call Sungard to officially declare a disaster using a CSC Authorization code.[15] Personnel from Sungard will validate the disaster declaration by calling one of the individuals on the Disaster Declaration Authorization Profile maintained by the VDC. Once Sungard receives a validation from authorized CSC management, they will confirm that the Sungard facility will be turned over to VDC personnel within 24 hours.

Throughout the entire disaster recovery effort, all recovery team members will maintain a log. The log will be used to document the status of ongoing recovery activities of each functional support group, and to document significant problems or issues encountered during the recovery effort. At a minimum, the log will contain the status of the following information:

- Secure disaster site
- Declare disaster
- Activate hot-site
- Retrieve data from off-site storage location
- Dispatch personnel to hot-site
- Activate telecommunication reserve lines
- Install new equipment at the hot-site
- Restore operating system
- Establish communications with users
- Restore databases
- Establish or reconstruct permanent facility
- Resume full processing at permanent site.

After normal operations are restored, the log will be used at debriefing sessions to determine the effectiveness of the plan and to identify any modifications that are needed. It will also be available for review by insurance company representatives during their investigations.

Recovery Site

Sungard Recovery Services Inc., located in North Bergen and Carlstadt, New Jersey, has been contracted as the hot-site vendor to support the configuration for the VDC. The mailing address for Sungard is as follows:

Sungard Recovery Services, Inc. (Mainframe site)
Computer Recovery Center
New York Metro System Center 2000
5851 West Side Avenue
North Bergen, NJ 07047

And

[15] Section extracted in part from VDC Disaster Recovery Plan for Midrange Systems dated March 8, 2002

Sungard Recovery Services, Inc. (Midrange site)
Computer Recovery Center
777 Central Blvd.
Carlstadt, NJ 07072

Offsite Storage
The off-site storage facility for system application/database backup files and supporting documentation is:

Iron Mountain
44 Griffin Road South
Bloomfield, CT 06002
203-243-9500
203-243-9338 (FAX)

All tapes are stored at Iron Mountain in areas known as “vaults." Tape backups of are stored in one vault while master files of critical applications required for service resumption are stored in another. The vault program is controlled by the tape management system or another system software used in each customer’s configuration. On a daily basis, newly created tapes are compared against a table containing vault information to determine if the tapes should be flagged to be sent off-site. If a tape requires off-site vaulting, information is written to a report that is used by the tape librarian to pull the tape and prepare it for shipment. Iron Mountain sends a bonded courier to the VDC daily to pick up and return tapes. Special aspects of a customer’s vault program can be found in customer unique disaster recovery plans. Only certain Data Center individuals have the necessary authorization to request tapes from off-site storage. In the event of a disaster, the Manager of Contingency Services or designee is responsible for authorizing the storage facility to ship the backup files to the hot-site facility. In addition to the backup tapes, a copy of the Tape Management System (TMS) Vault Inventory list, an Operation System Manual, a listing of all VDC employees' home telephone numbers and the Disaster Recovery Plan are stored at the off-site facility and will be shipped to the hot-site.

Appendix G contains a table describing the backup schedule for SAIG.

3.5 Reconstitution

In the reconstitution phase, recovery activities are terminated and normal operations are transferred back to the organization’s facility. If the original facility is unrecoverable, the activities in this phase can also be applied to preparing a new facility to support SAIG’s processing requirements. Until the primary system is restored and tested, the contingency system will continue to be operated.

3.5.1 Continuity of Support Reconstitution

The CSC SRT has the lead role reconstituting SAIG. Regardless of the event, from sprinkler failure to hardware failure, CSC reconstitution procedures govern the process. Below is a summary list of the steps CSC may employ to resume normal SAIG operations at the VDC:

- Clean up damaged site

- Coordinate insurance claims for damaged property
- Coordinate media release
- Reestablish or reconstruct permanent facility
- Maintain special purchase orders for restoration expenses
- Procure all materials and services required to repair damages
- Coordinate all reconstruction activities for damaged facility
- Coordinate repair/replacement of hardware
- Coordinate repair/replacement of communications networks
- Coordinate with voice communication companies as required
- Restore operating system software
- Resume SAIG processing at VDC.

.

3.5.2 Disaster Recovery Reconstitution

This section discusses activities necessary for restoring SAIG operations at the original or new site. When the computer center at the original or new site has been restored, SAIG operations at the alternate site must be transitioned back. The goal is to provide a seamless transition of operations from the alternate site to the computer center.

To transition back to the VDC or the new site, SAIG will proceed through three phases: original/ new site processing, concurrent processing, and finally plan deactivation.

Procedures to return to the VDC are the reverse of the disaster recovery procedures to implement processing at an alternate location.[16] These procedures include the following activities:

- Develop a detailed plan to switch processing back to the VDC facility.
- Phase VDC personnel back into normal operating schedules at the restored Meriden facility.
- Return VDC data from the hot-site or alternate storage facility to Meriden or return to the off-site storage facility.
- Terminate leasing arrangements at the hot-site for office equipment, supplies, CRTs, alternate vault or storage facilities.
- Update equipment tracking database to reflect equipment removal/replacement.
- Submit expense reports to validate disaster recovery related expenditures.

CSC will conduct tests of the original/new facility to ensure the following:

- Availability of required host connectivity,
- Server capability, and
- The SAIG system has been restored to the appropriate LAN.

When normal operations have resumed at the VDC, or application processing is implemented at the hot-site location, the Service Restoration Team Chairperson will call a debriefing of all members of the SRT and Disaster Recovery Teams. At this meeting, initial response, disaster recovery procedures and recovery logs will be reviewed. Procedures that can improve or add

[16] Section extracted in part from VDC Disaster Recovery Plan for Midrange Systems dated March 8, 2002

efficiency to the Disaster Recovery Plan will be assigned to appropriate team members for investigation and future inclusion into the plan.

PLAN APPENDICES

The following appendices are included with this plan:

- *CSC Team Functions and Responsibilities*
- *Personnel authorized to declare a disaster*
- *SAIG Test Plan*
- *SAIG Logical Diagram*
- *Business Impact Analysis*
- *Personnel Contact List*
- *SAIG Backup schedule*.

This plan also references several other documents that are not included within this plan, such as the VDC Midrange Disaster Recovery Plan. For these documents, please contact the document owner directly.

APPENDIX A - CSC TEAM FUNCTIONS

This appendix is extracted from the VDC Midrange Disaster Recovery Plan. Its contents are included in the SAIG COS/DR to give additional transparency to the VDC recovery activities.

SERVICE RESTORATION TEAM RESPONSIBILITIES

The Service Restoration Team's responsibilities during the initial response to a disaster (first 6 hours) include the following:

- Activate emergency and evacuation plans, if not already activated
- Notify appropriate departments (security, fire and maintenance)
- Complete a brief evaluation of injury to personnel and damage to facility (within 1 to 2 hours after a disaster occurs)
- Establish command center if necessary
- Notify CSC Headquarters
- Notify Account Representatives
- Notify hot-site to be on stand-by
- Notify off-site storage facility to be on stand-by
- Notify telecommunications provider to be on stand-by
- Complete the preliminary assessment of damage
- Declare disaster mode and activate the Disaster Recovery Plan
- Notify remaining Disaster Recovery Team members
- Monitor the recovery team's execution of recovery procedures and resolve conflicts/problems as needed.

Concurrent with performing their initial evaluation, SRT members are also responsible for initiating and monitoring recovery tasks assigned to their functional areas. When the initial evaluation of the damage has been completed and the Data Center Manager declares a disaster, the team members continue their duties as Disaster Recovery Team members.

The VDC has an Emergency and Evacuation Plan. Disaster Recovery procedures are based on the assumption that these plans have been initiated or completed. If not already activated and, if necessary, the Meriden Director of Human Resources activates the Emergency and Evacuation Plan.

The names and phone numbers of all members of the VDC Service Restoration Team, Disaster Recovery Team and other key personnel requiring immediate notification are contained in the VDC midrange DR Plan. In addition, a list of all Meriden employees, with home phone numbers, is kept at the off-site storage facility with a copy of the Disaster Recovery Plan for use by the SRT. This list may be used after the Meriden Service Delivery Manager or an alternate has officially declared a disaster, or when there is a need to notify specific employees and provide them with information and/or instructions pertaining to the emergency.

CSC Human Resources will call the local media to handle the notification of all employees only after receiving authorization from CSC Headquarters.

SRT members complete a preliminary assessment and submit a report to the Meriden Service Delivery Manager who will make the decision whether or not to implement the recovery procedure. This report may be verbal in order to get the information to the Meriden Service Delivery Manager as soon as possible, but cannot exceed four (4) hours from point of disaster. All verbal reports must be followed by a written report when time permits. After the preliminary report is completed, SRT members (or their delegates) continue to complete a detailed analysis of damage to the VDC to determine the equipment and facilities that must be repaired and/or replaced.

The damage assessment report includes (but is not limited to) the following:

- Brief description of the disaster, including the date, time, type of occurrence (fire, earthquake, etc.) and cause (accidental or intentional)
- Number of injured and deceased employees
- Amount of damage to electrical, environmental or water systems
- Amount of damage to security or fire detection systems
- Amount of structural damage
- Amount of processing equipment damaged
- Amount of teleprocessing equipment damage (terminals, modems, cables, etc.)
- Estimated timeframe to repair or replace minimum hardware required to restore processing at the damaged site (if possible)
- Estimated timeframe to repair or replace minimum teleprocessing equipment required to support processing at the damaged site (if possible)
- Estimated timeframe to restore the damaged site to full operating capacity
- Recommendation on the disaster mode
- Recommendation on activation of the hot-site
- Estimated timeframe to migrate to the hot-site and become operational
- Estimated costs of processing applications at the hot-site (i.e. shipping of printed reports, outsourcing microfiche)
- Estimated cost of repairing and/or replacing damaged computer and teleprocessing equipment
- Estimated cost of restoring or reconstructing the damaged facility, including the possibility of reconstruction at a new location.

DISASTER RECOVERY TEAM RESPONSIBILITIES

The Disaster Recovery Team is responsible for implementing recovery procedures after the Meriden Data Center Manager formally declares a disaster and activates the Disaster Recovery Plan. Team members must keep the DRT Chairperson and their SRT members informed of the status of recovery activities for their areas and immediately report any potential problems.

Subsections 2.1 - 2.7 list the responsibilities of each Disaster Recovery Team member in being prepared for a disaster, in assessing damage if a disaster occurs and reporting the assessment to the SRT. Also listed are the actions and responsibilities of each team member to restore services at the current facility or backup site based on the disaster mode in effect.

2.1 CSC Technical Team

CSC team members include the Manager of Technical Operations (TO), the Operations Lead (OPS), the Manager of Contingency Services (CS), the Manager of Teleprocessing (TP) and key technical systems and network personnel from CSC.

It is the responsibility of the CSC Technical Team to initiate and maintain system information that would be required in system recovery as part of normal operating procedures. The following list highlights key actions that functional areas within CSC perform.

- Ensure that required operating systems are backed up to tape and stored at the off-site facility (TO, OPS)
- Maintain an updated hardware configuration for each customer and/or mainframe (TO)
- Maintain a hardware configuration of equipment that will be required at the recovery site (CS)
- Maintain DASD configurations for each system (TO)
- Maintain a configuration of critical software with release numbers (TO, TP)
- Maintain a configuration of software with local modifications that will be required at the recovery site (TO, TP, CS)
- Maintain updated vendor manuals for critical hardware and software, and ensure that they will be available at a recovery site (ALL)
- Maintain network recovery procedures and configurations (TO, TP)
- Ensure that all tapes that must be off-site are stored as scheduled (OPS)
- Maintain contract for hot-site services (CS)
- Maintain Operations manuals for each customer (OPS)
- Maintain the Disaster Recovery Plan telephone directory (SFA Manager of Contingency Service).

Technical support members work together with vendor representatives to determine the amount of damage to computer hardware (mainframe and peripherals) and teleprocessing equipment (cables and links). The Data Center Manager (or delegate) makes the initial contacts to hardware vendors.

Preliminary Damage Assessment Report identifies:

- Extent of damage to equipment and the amount of computer and communications processing capability (if any) remaining
- How long it will take to restore the damaged Data Center to normal operating conditions
- Recommendation on whether or not to activate the hot-site.

Detailed Damage Assessment Report contains:

- List of equipment that can be repaired in less than 24 hours
- List of equipment that can be repaired within 24 to 48 hours
- List of equipment that will take longer than 48 hours to repair
- List of new equipment that must be acquired with estimated arrival dates.

After the Meriden Service Delivery Manager (or delegate) develops the preliminary report, a report is submitted with appropriate forms and cost estimates to receive approvals to acquire replacement equipment.

The Data Center Manager functions as the on-site VDC Disaster Recovery Project Manager. The local CSC team is responsible for the following functions:

- Initiate procedures to restore the damaged site to normal operating mode
- Restore all Operations functions at the damaged site
- Ensure other network related and remote equipment is functioning
- Ensure that an adequate source and/or inventory of supplies and scratch tapes are available
- Initiate and maintain Production Control and Operations during a disaster recovery period either at the damaged site or the command center
- Coordinate the recovery of the network between Meriden and customer sites.

The Manager of Contingency Services functions as the hot-site Disaster Recovery Project Manager. The CSC team at the hot-site is responsible for the following functions:

- Initiate contact with Sungard to declare a disaster and inform Sungard of arrival time at hot-site
- Initiate contact with software vendors to obtain CPU codes to process on alternate mainframes
- Notify the off-site storage facility to ship back-up/recovery material to the hot-site
- Initiate and maintain all hardware/software functions required for processing at the hot-site
- Inventory material received from Iron Mountain
- Initiate and maintain activities required to restore and activate database processing
- Coordinate all activities necessary to support recovery of databases at the hot-site
- Create a tape-library at the hot-site and arrange for local off-site storage
- Implement Operations at the hot-site
- Initiate and maintain Production Control and Operations during the disaster recovery period at the hot-site
- Ensure that an adequate source and/or inventory of supplies and scratch tapes is available at the hot-site
- Coordinate the recovery of the T1 network between Sungard and customer sites
- Ensure that any network-related equipment is functioning
- Coordinate food/lodging and other essentials for CSC staff.

2.2 CSC Facility Team

The Facility Team is responsible for the physical structure and environment support systems at the VDC.

Facilities personnel routinely check the functionality of environmental alarms and alternate power generation. They are also responsible for building maintenance and repair on an on-going basis and maintain purchase orders with local vendors to support the building and its operations.

The Facility Team's first priority is to assess damage to the VDC structure and support systems as quickly as possible. Facilities staff will work closely with the personnel from the fire, security and maintenance departments to determine if the facility can be entered safely. All team members must first check with Security for clearance for themselves or their staff to enter a damaged area. The Facility team SRT member reports to the Meriden or civil emergency authorities in charge before entering a damaged area and before starting an on-site evaluation. The Facility team SRT member will obtain all or some of the following emergency equipment before entering a damaged area: hard hat, rubber boots, radio, insulated gloves, safety glasses, waterproof pad and writing instrument. The Facility team SRT member will perform an exterior inspection of the damaged area and shut off electrical feeders if necessary before performing an inspection of the interior of the damaged facility. The Facility SRT member completes the following checks as quickly after the occurrence of the disaster to enable the VDC Manager of Contingency Services to determine the disaster mode and to decide if the hot-site is to be used.

- Electrical equipment
- Structural damage
- Water systems
- Power source machinery
- Fire detection systems
- Environment support systems
- Security (Alarm) system.

These checks are reviewed in detail after the preliminary damage assessment report has been completed. The detailed report from the Facility Disaster Team will contain realistic time and cost estimates for necessary repair and/or reconstruction work. Section 3.5 contains a list of contractors that can be used by the Facility Team to assess the damages.

The following are the actions and responsibilities of the Facility Team:

- Determine the extent of damage to VDC facility and its utility and environmental support systems
- Determine if power generators or other equipment will be needed on a temporary basis
- Determine which equipment can be repaired and what needs to be replaced
- Determine which equipment can be rented or leased
- Determine if Halon and sprinkler systems are functioning or should be deactivated
- Determine if security alarms are functioning or make arrangements for alternate security measures
- Determine if telephone communications lines are functioning and report this information to the CSC Disaster Recovery Team members
- Coordinate activities with Meriden Department of Public Utilities
- Coordinate repair or reconstruction activities to the Meriden facility

- Contact facility contractors to repair or reconstruct the Meriden facility, if required
- Contact CSC Purchasing to arrange for temporary office space, if required
- Coordinate support including supplies, deliveries to and from the damaged site and required support personnel
- Determine if temporary trailers are required to house office personnel and proceed accordingly
- Coordinate with the Director of Security to determine if damage has any physical security ramifications.

2.3 CSC Security Team

The Security Team is responsible for the protection of personnel and property from injury or further damage and to ensure that safeguards are in place to prevent unauthorized access to the facility and disclosure of or access to data.

Ensure that physical security at the damaged site is adequate to protect CSC personnel and assets and coordinate with Facility Team members to ensure safe access.

The following are the actions and responsibilities of the Security Team:

- Prevent unauthorized access to data at the damaged site. Implement the disaster mode of the physical access control system to allow only authorized Disaster Recovery Team members and staff entry into the damaged VDC site. If the access control system is not operational, a list of personnel authorized to access the data center is given to the subcontracted security personnel
- Recall all available guard force and security personnel and set up guard stations where appropriate
- Request/notify outside assistance where applicable, (i.e. Police, FBI, Pinkerton, etc.)
- Secure affected areas and ensure that perimeter barriers are in place at all facility entrances/exits
- Coordinate the relocation of usable equipment to secure areas
- Coordinate the installation and maintenance of the VDC data security function at the damaged facility or backup site.

2.4 CSC Human Resources Team

The Human Resources Team is responsible for any personnel issues that may arise in the VDC.

Human Resources personnel are responsible for maintaining a complete list of VDC employees working in alternate locations. This information includes name, address, telephone number, name and telephone number of person to call in case of an emergency.

A Human Resources SRT member will be involved in the initial evaluation phase of recovery procedures if there are personnel injuries or fatalities.

The Human Resources Disaster Recovery Team member's responsibilities include:

- Activate Emergency and Evacuation Plan, if required

- Coordinate with CSC Headquarters personnel for the notification of immediate family of injured or deceased employees
- Handle all media and public relations contacts when authorized by CSC Headquarters
- Interface with other CSC Data Centers for availability of key personnel, if required.

2.5 CSC Finance Team

The Finance Department is responsible for handling all monetary issues relating to the VDC. Certain of these activities are performed in total in Meriden, while others are performed in other CSC locations.

The Finance Department has procedures that allow alternate CSC locations to handle financial matters. These matters involve purchasing/leasing assets, bill payment, personnel expense related issues, creating and dispersing paychecks, etc.

The Finance member of the SRT is responsible for assisting the CSC Teams in developing financial cost estimates for the damage assessment report.

Once a disaster has been declared, the Finance disaster recovery team responsibilities will include:

- Monitor all disaster recovery-related expenses and labor charges
- Procure construction and maintenance services, supplies and equipment as needed to repair or restore the damaged VDC.

2.6 CSC Account Management

A senior CSC official (president of GIS) has overall responsibility for all customer accounts. He performs this function in conjunction with a Regional Account Executive and Customer Account Managers.

Account Managers are responsible for reviewing disaster recovery plans with their clients and ensuring that contractual obligations regarding disaster recovery are met.

Account Management will work with clients to understand the specific impact on a client's business.

The Account Manager is responsible for the following functions:

- Notify Customer's Senior IS and Management staffs
- Ensure Information Resource Directors/Managers are notified and informed of the status.

2.7 CSC Vendor Representatives

The VDC has customer engineers on-site. In addition, vendors on a pre-scheduled basis perform regular maintenance activities. Preventive maintenance is performed on equipment where applicable. Monday through Friday, error logs on all customer systems are reviewed for potential problems. Vendors will work with the CSC Teams to assist in documenting the extent of damage to the VDC.

Representatives of the major hardware vendors will provide assistance, as required, in the following manner:

- Replace hardware as quickly as possible.
- Restore operations at the damaged VDC, if possible.

APPENDIX B - PERSONNEL AUTHORIZED TO DECLARE A DISASTER

Only the following people are authorized to declare a disaster and move VDC and SAIG operations to the Sungard Recovery Facility:

NAME: JIM O'DONNELL
TITLE: CONTINGENCY SERVICES MANAGER
ADDRESS: 55 Capital Blvd. 2nd Floor
Rocky Hill, CT 06067
PHONES: (Work, Fax, Home, Cellular)
860-513-5845
860-257-6149
860-621-4671
860-212-5741
PERSONAL DDA CODE NONE
PRIMARY CONTACT TO DECLARE DISASTER: YES

NAME: GLEN BENTON
TITLE: CONTINGENCY SERVICES MANAGER
ADDRESS: 6100 WESTERN PLACE
FORT WORTH, TX. 76107
PHONES: (Work, Fax, Home, Cellular)
817-782-0822
817-762-8690
817-295-7360
817-317-3862
PERSONAL DDA CODE NONE

NAME: COSETTE HEIMANN
TITLE: CONTINGENCY SERVICES MANAGER
ADDRESS: 55 Capital Blvd. 2nd Floor
Rocky Hill, CT 06067
PHONES: (Work, Fax, Home, Cellular)
860-513-5853
860-257-6149
860-457-1539
1-800-216-3133 pin 5981862
860-978-7594
PERSONAL DDA CODE NONE

NAME: MICHAEL SUMMERS
TITLE: CONTINGENCY SERVICES MANAGER
ADDRESS: 500 CREEK VIEW ROAD, 4TH FLOOR (4W42)
NEWARK, DE. 19711
PHONES: (Work, Fax, Home, Cellular)
302-391-8754
302-391-8446

610-565-9734
302-559-0406
PERSONAL DDA CODE NONE

NAME: THOMAS CARROLL
TITLE: DIRECTOR, BUSINESS CONTINUITY
ADDRESS: 23 Wall Street 23/15B
NY, NY 10260
PHONES: (Work, Fax, Home, Pager, Cellular)
631-757-1280
631-757-7787
631-757-6651
917-545-9552
917-545-9552
PERSONAL DDA CODE NONE

NAME: THOMAS COX
TITLE: DIRECTOR OF OPERATIONS
ADDRESS: 100 WINNENDEN ROAD
NORWICH, CT. 06360
PHONES: (Work, Fax, Home, Pager, Cellular)
860-859-4859
860-533-9380
248-363-5988
888-501-5857
203-631-0163
PERSONAL DDA CODE: NONE

NAME: JEFF ANDREW
TITLE: VP GLOBAL OPERATIONS
ADDRESS: 645 PAPER MILL RD.
ROOM 1079
NEWARK, DE 19711
PHONES: (Work, Fax, Home, Cellular)
302-292-9543
302-292-9749
248-363-5988
302-521-3087
PERSONAL DDA CODE: NONE

APPENDIX C – SAIG TEST PLAN

CSC

PROJECT AUTHORIZATION DOCUMENT

Project Name: Hotsite Disaster Recovery Test for SAIG Enrollment, FSA Download and SAIG Mailboxes, November 12th , 2002

Project Manager: Maria Cullen, CSC

Project Sponsor: Lydia Morales, Department of Education, FSA

Description of Work to be Performed

This project is a hotsite disaster recovery test that will be conducted by CSC at the SunGard hotsite recovery facility in Carlstadt, New Jersey. This will be a recovery test of the SAIG Enrollment, FSA Download, and SAIG Mailboxes and the Production systems residing on HP and NT servers. The HP midrange recovery will begin at 0800 hrs, November 12th, and will end no later than 0800 hrs, November 14st. This HP recovery test will be a "48 hour" test. The NT midrange recovery will begin at 2400 hrs, November 12th and will end no later that 0800 hrs, November 14st. This NT recovery test will be a "32 hour" test. .

Primary Test Objectives *Primary objectives are essential for the success of the recovery test.*

1. Verify that all resources required for recovery reside in offsite vault.
2. Verify that all tapes required to restore/recover the SAIG HP midrange production systems are successfully transported to SunGard in NJ from Iron Mountain in CT.
3. Verify that all tapes required to restore/recover the SAIG NT midrange production systems are successfully transported to SunGard in NJ from Iron Mountain in CT.
4. Restore the SAIG Mailboxes (B-Trade) HP system residing on HPL16 and its associated data using the full volume backups from October 27th .
5. Restore the FSA Download (SAIGFTP) NT system residing on SFANT007 and the associated data using the full volume backups from October 27th.
6. Restore the SAIG Enrollment (SAIGPROD) NT systems residing on SFANT007 and the associated data using the full volume backups from October 27th.
7. Restore the SAIG Mailboxes (FSA on the Internet, B-Trade) NT system residing on SFANT014 and its associated data using the full volume backups from October 27th.
8. Provide network connectivity to Iowa City from the FSA Download NT system that will be recovered at the SunGard facility in Carlstadt, NJ.
9. Provide network connectivity to Union Center Plaza (UCP/ROB3) from the FSA Download NT system that will be recovered at the SunGard facility in Carlstadt, NJ.
10. Provide network connectivity to Iowa City from the SAIG Enrollment NT system that will be recovered at the SunGard facility in Carlstadt, NJ.
11. Provide network connectivity to Union Center Plaza (UCP/ROB3) from the SAIG Enrollment NT system that will be recovered at the SunGard facility in Carlstadt, NJ.
12. Provide network connectivity to Union Center Plaza (UCP/ROB3) from the SAIG Mailboxes (FSA on the Internet) that will be recovered at the SunGard facility in Carlstadt, NJ.
13. Provide Internet connectivity to www.SAIGPortal.dr.sfa.ed.gov from the SAIG Mailbox server that was recovered at the SunGard facility in Carlstadt, NJ.
14. Provide Internet connectivity to www.sfadownload.dr.ed.gov from the FSA Download server that was recovered at the SunGard facility in Carlstadt, NJ.
15. Provide Internet connectivity to www.sfawebenroll.dr.ed.gov from the SAIG Enrollment server that was recovered at the SunGard facility in Carlstadt, NJ.
16. Init all DASD volume's at end of test.

Secondary Test Objectives *Secondary objectives are additional goals that would be beneficial to the program.*

FSA to the Internet:

1. Navigate the web site www.SAIGPortal.dr.sfa.ed.gov from UCP/ROB3.

2. Access the data in the SAIG database on the HPL16 server from UCP/ROB3.

FSA Download:

1. Navigate the web site www.sfadownload.dr.ed.gov from UCP/ROB3.

Web Enrollment:

1. Navigate the web site www.sfaenrollment.dr.ed.gov from UCP/ROB3.

CSC may have additional primary or secondary objectives that are not in the scope of this client project.

Client Approval

Name (print):_____ Signature:_____ Date:_____

Account Manager Approval

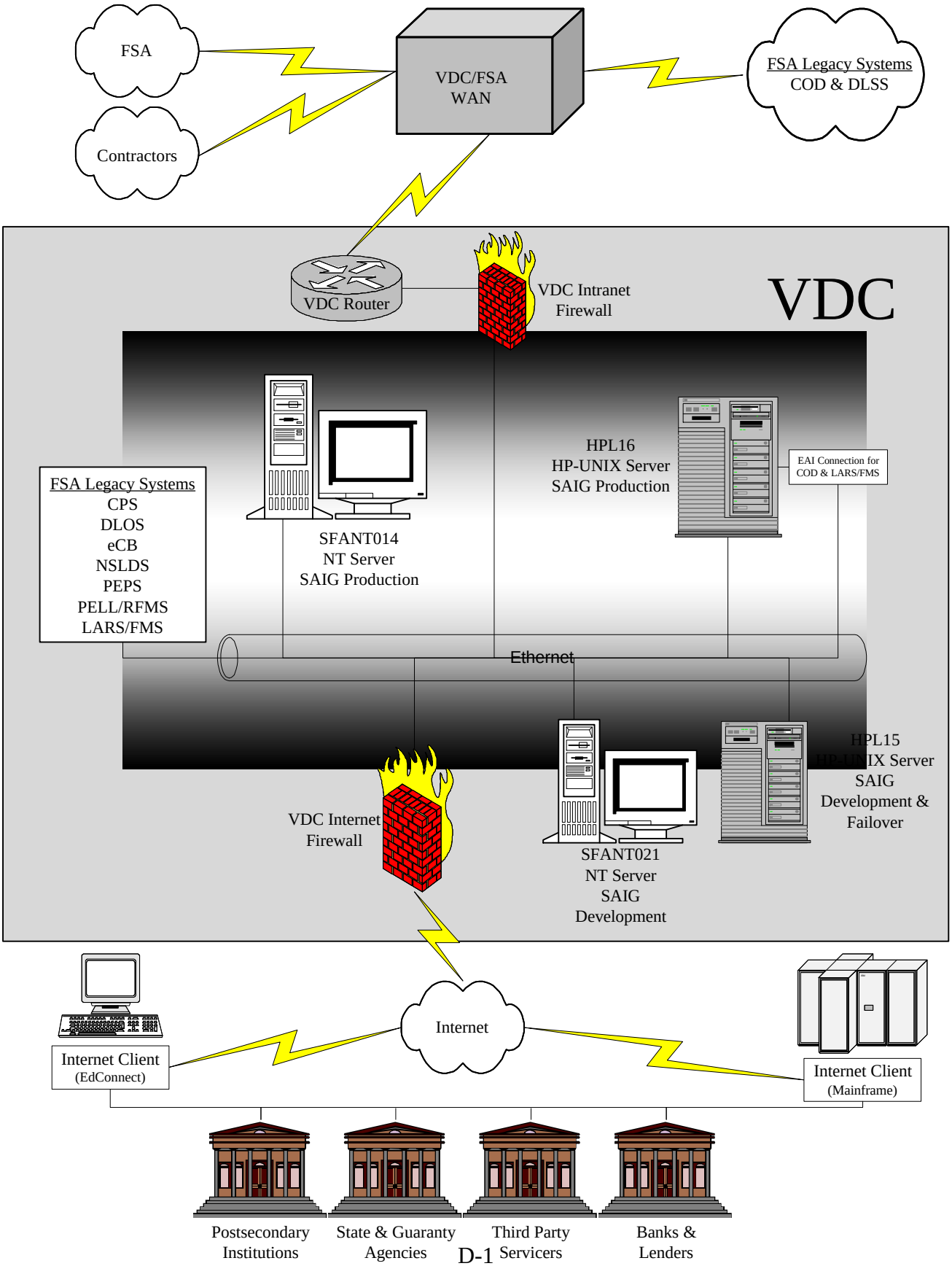
Name (print):_____ Signature:_____ Date:_____

Service Delivery Manager Approval

Name (print):_____ Signature:_____ Date:_____

Approvals may be via email. Reference the Project Name in the approval.

APPENDIX D - SAIG LOGICAL NETWORK DIAGRAM



APPENDIX E - BUSINESS IMPACT ANALYSIS

Preliminary System Information

Organization: FSA	Date BIA Completed: Nov. 20, 2002
System Name: Student Aid Internet Gateway (SAIG)	BIA POC: Colleen Ward
System Manager Point of Contact (POC): Lydia Morales	

System Description:

The Student Aid Internet Gateway (SAIG) Portal provides telecommunications support for the delivery and administration of Title IV programs via the Internet. The U.S. Department of Education (ED) and its Integration Partners Accenture and NCS Pearson are sponsoring the SAIG Portal to promote the electronic exchange of Title IV information between differing educational and other types of entities over the Internet.

SAIG Portal's core is composed of an HP-UNIX midrange that supports the mailboxing system and an NT/IIS server running a Web administrative application. Supplementary systems include: mainframe, enrollment Web application, and PC systems. The SAIG Portal is a Commercial Off-the-shelf (COTS) application from bTrade.com and is made up of the following core components:

- Transaction Delivery Engine (TDN) – An open architecture gateway used as the "mailbox" application for the storage and retrieval of data
- TDAccess – The client software used to send/receive (FTP) FSA data transmissions securely over the Internet using Secure Sockets Layer (SSL) 3.0 and the Diffie-Hellman Dynamic Key Exchange algorithm
- Transaction Delivery Manager (TD Manager) – Product used to manage Title IV destination point mailboxes and data. The online software is referred to as Transaction Delivery Community Manager (TDCommunityManager or TDCM).

These core components of the SAIG Portal are run from the Virtual Data Center (VDC) in Meriden, Connecticut. Computer Sciences Corporation (CSC) staff are responsible for the operation, maintenance, and security of this system from a hardware and operating system perspective, with the support of Accenture and NCS Pearson staff for application administration and maintenance.

A. Identify System POCs	**Role**
Internal	
• Baha Shehata • Lydia Morales • Tawanda Hampton	• SAIG System Manager • SAIG Technical Lead • SAIG System Security Officer – maintain security documentation

• Colleen Ward • COD • CPS • DLOS • DLSS • eCB • FMS/LaRS • NSLDS • RFMS (PELL)	• Mod Partner Manager for SAIG • These systems, within the FSA organization, exchange Title IV information through SAIG.
• CPS/PM	• Provides userIDs for new, participating organizations.
External	
• CSC	• Maintain and operate Virtual Data Center; provide hosting hardware for SAIG software
• Mod Partner	• Develop and maintain SAIG software; operate and host SAIG Enrollment
• Guaranty Agencies • Education Institutions • Lenders • State Agencies	• These institutions exchange Title IV information via SAIG.
B. Identify System Resources	
Hardware • HPL16 • SFANT014 • HPL15 (Development) • SFANT021 (Development)	
Software • Oracle Database v8.1.7 • MQ Series Server v5.2 • bTrade EAclient API • HP-UX v11.0 • Computer Associates TNG • Cisco Local Director • HP Service Guard • SecureManager 2000 • Oracle Application Server • Online SecureManager Software • JDK (Java Development Kit) • Java Mail • JAF (Java Activation Framework)	

• JRUN (Enterprise Edition) • CA-TNG Monitoring Agent • Tripwire Client • ArcServe Client • Norton Antivirus	

C. Identify critical roles

- CSC - Maintenance and operation of Virtual Data Center; provide hosting for SAIG hardware and software
- Integration Partner – Development and maintenance of SAIG bTrade software
- All systems, schools Guaranty Agencies, etc. exchange Title IV information via SAIG.

D. Link critical roles to critical resources

Critical Role	Critical Resources
Maintain and operate Virtual Data Center; provide hosting for SAIG hardware	• HPL16 • SFANT014 • HPL15 (Development) • SFANT021 (Development)
NCS Pearson – Development and maintenance of SAIG software	• HPL15 (Development) • SFANT021 (Development) • bTrade Software
All systems, schools and GAs exchange Title IV information via SAIG.	• HPL16 • SFANT014 • bTrade Software

E. Identify outage impacts and allowable outage times

Resource	Outage Impact	Allowable Outage Time
HPL16	• Customers unable to access Mailbox and deliver/receive Title IV information	• **2-4 hours**
SFANT014	• Customers unable to access TDCM and view current/pending transaction.	• **24-48 hours**
HPL15	• Fail over, Development, and Test server. Cannot restore production server if backup is unavailable.	• **8-12 hours**

SFANT021	• Fail over, Development, and Test server. Cannot restore production server if backup is unavailable	• **72 hours**
bTrade Software	• Failure to maintain appropriate patches and updates to bTrade software could degrade the integrity of SAIG processing	• **Zero outage is acceptable. Software must be current and installed properly on associated hardware.**

F. Prioritize resource recovery

Resource Recovery	Priority
HPL16	1
HPL15	2
SFANT014	2
SFANT021	3
bTrade Software	4

APPENDIX F - SAIG CONTACT LIST

Modified 11-7-02

Name	Function	Email	Telephone
Lydia Morales	FSA Sponsor	Lydia.Morales@ed.gov	202-377-3589
Tawanda Hampton	FSA- SAIG SSO	Tawanda.Hampton@ed.gov	202-377-3575
Baha Shehata	FSA	Baha.Shehata@ed.gov	
Denise Barnes	FSA	Denise.Barnes@ed.gov	202-377-3576
James Cunningham	FSA VDC SSO	james.cunningham@ed.gov	202-377-3577
Gail Gurley	FSA	gail.gurley@ed.gov	202-377-3588
John Hsu	FSA – DNS Mgr.	John.hsu@ed.gov	202-377-3579
Colleen Ward	Accenture	Colleen.m.ward@accenture.com	703-947-2980
Dale McKeag	NCS Pearson	Dale_ McKeag@ncs.com	319-665-7986
Deb Sheets	NCS Pearson	Sheede@ncs.com	319-665-7882
Jamie Steapp	NCS Pearson	Jamie_ Steapp@ncs.com	319-665-7987
Martin Happ	NCS Pearson	happma@ncs.com	319-665-7847
Yanhua Wu	NCS Pearson	WUXXYa@ncs.com	319-665-7862
Benji Bondoc	Network Support	bbondoc@csc.com	203-317-5132/ 860-513-2354
Benson P Hwang	NT Support	bhwang@csc.com	203-317-4895
Craig Gates	NT Support	cgates3@csc.com	203-317-5174
David Mlynek	Unix Support	dmlynek@csc.com	860-290-0873
Janette Brogan	Unix Support	jbrogan@csc.com	203-317-4824
Jean Langevin	NT Support	jlangev1@csc.com	203-317-4864
Jim O'Donnell	CSM	Jodonn21@csc.com	860-513-5845
Kris Strubell	Network Support	kstrubel@csc.com	203-317-5215
Maria Cullen	CSM Team Lead	mcullen2@csc.com	860-513-5864
Paul Izzo	Unix Support	pizzo@csc.com	203-317-2175
Cheryl Teart	Tape Ops Supervisor	cteart@csc.com	203-317-5069
Dave A Barber	GPES Mgr.	dbarber7@csc.com	203-317-4899
Dave Hugh	Network Manager	Dhugh@csc.com	203-317-5006
Dave Lass	Service Delivery Manager	dlass@csc.com	203-317-5037
David Barber	Mgr. HP Support	dbarber7@csc.com	203-317-4899 / 860-291-5962
Gary Adams	Service Delivery Manager	gadams2@csc.com	202-842-8614
John Pilla	Availability Manager	jpilla2@csc.com	203-379-5220
Paul Noniewicz	Unix Team Leader	pnoniewi@csc.com	860.823.2109
Jeff Robinson	Account Executive	jrobin13@csc.com	240-456-6153
Jerry Ryznar	Account Executive	gryznar@csc.com	240-456-6412 /202-842-7397
Larry Hale	NT Manager	lhale3@csc.com	203-317-4821
Lisa Hart	Ops Manager	Lhart2@csc.com	203-317-5137
Lisa Tabor	Unix Support Team Lead	ltabor2@csc.com	302-391-8498 / 609-726-0153

APPENDIX G – SAIG BACKUP SCHEDULE

Backup Job Name	Day	Type	Application Status	Start Time	End Time	File Systems Backed-Up	Purpose	Retention Weeks
hpl16.oracle	Sunday	Full	down	3:00	4:40	/u01 ./u02 /u03 /u04 /u05 /var/mqm	weekly full backup eaibus data	26
hpl16.oracle.daily	Mon-Sat	Fulll	up	5:00	5:49	/dbbackup /arch	Daily Oracle backup, roll forward recovery	26
hpl16_eaadmin	Saturday	Full	up	22:45	2:44	/eaadmin	weekly full backup of brade data	26
hpl16.eaadmin.data.bk	Mon-Sat	Incremental	up	1:45	2:08	/eaadmin /var/mqm /ex[port/data/mqm	daily incremental of btrade and eaibus data	26
hpl16_arch	Sun	Full	up	12:00	20:36	/eaadmin/archive /export/data/mqm	Weekly full backup of btrade archive data and eibus data	26
hpl16_arch	Mon-Sat	Incremental	up	6:00	7.26	/eaadmin./archive /export/data/mqm	daily incremental backup of btrade archive data and eaibus data	26
hpl16	Sunday	Full	up	21:00	21:43	/ /usr /opt /tmp /var /stand /home	weekly full operating system backup	26

						/opt/odbc /var/spool/cron/crontabs /opt/mqm /home/mqm		
hpl16	Mon-Sat	Incremental	up	21:00	21:19	/ /usr /opt /tmp /var /stand /home /opt/odbc /var/spool/cron/crontabs /home /home/mqm	daily incremental operating system backup	26
btrade.make_recovery	Saturday	Full	up	14:00	16:20	vg00	operating system disaster recovery tape	4